Le parole del *cyber*

0-day. Qualsiasi vulnerabilità non nota e relativo attacco informatico che la sfrutta.

Advanced Persistent Threat **(APT)**. Minaccia consistente in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti bersaglio al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle reti dell'ente obiettivo.

Attribution. Termine che identifica l'attribuzione di una specifica minaccia *cyber* come, ad esempio, una campagna di *cyber*-spionaggio, ad un determinato attore ostile.

Bring Your Own Device **(BYOD)**. Insieme di *policy* interne ad un'organizzazione, sia essa pubblica o privata, volte a regolare l'impiego di dispositivi digitali personali all'interno della stessa, da parte dei relativi dipendenti.

Cybercrime-as-a-Service. Fornitura, da parte di gruppi criminali, di servizi e prodotti, solitamente acquistabili sul mercato nero digitale, utilizzabili da parte di terzi al fine di sferrare attacchi informatici. Tra i "beni" commercializzati figurano *exploit kit*, *malware*, nonché piattaforme da usare per la raccolta di materiale illegale od oggetto di indebita acquisizione.

Distributed Denial of Service **(DDoS)**. Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (*botnet*), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi *server*.

DNS Poisoning. Noto anche come *DNS Cache Poisoning*, è la compromissione di un server *Domain Name System* (DNS) comportante la sostituzione dell'indirizzo di un sito legittimo con quello di un altro sito infettato dall'attaccante.

Domain Name System **(DNS)**. Sistema per la risoluzione di nomi dei nodi della rete (cd. *host*) in indirizzi IP e viceversa.

Exploit. Codice che sfrutta un *bug* o una vulnerabilità di un sistema informatico.

Hacktivista. Termine che deriva dall'unione di due parole, *hacking* e *activism* e indica chi pone in essere le pratiche dell'azione diretta digitale in stile *hacker*. Nell'ambito dell'*hacktivism* le forme dell'azione diretta tradizionale sono trasformate nei loro equivalenti elettronici, che si estrinsecano prevalentemente, ma non solo, in attacchi DDoS e *web defacement*.

Indicators of Compromise **(IoC)**. Indicatori impiegati per la rilevazione di una minaccia nota e generalmente riconducibili ad indirizzi IP delle infrastrutture di Comando e Controllo (C&C), ad *hash* (MD5, SHA1, ecc.) ai moduli del *malware* (librerie, *dropper*, ecc.).

Industrial Control System **(ICS)**. I sistemi di controllo industriale includono i sistemi di controllo di supervisione e acquisizione dei dati (*Supervisory Control and Data Acquisition*-SCADA), i sistemi di controllo distribuiti (*Distributed Control Systems*-DCS) e i controllori a logica programmabile (*Programmable Logic Controller*-PLC), impiegati usualmente negli impianti industriali.

Ingegneria sociale. Tecniche di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Internet of Things (IoT). Neologismo riferito all'interconnessione degli oggetti tramite la rete Internet, i quali possono così comunicare

dati su se stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di impiego sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

Malware. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati. Non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare vulnerabilità non ancora note (cd. *0-day*) per infettare le risorse informatiche dei *target*. Ciò consente a tali *software* di non essere rilevati dai sistemi antivirus e di passare praticamente inosservati. Essi, inoltre, sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete generato dall'ordinaria attività lavorativa del *target*.

Ransomware. *Malware* che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I *ransomware* sono, nella maggioranza dei casi, dei *trojan* diffusi tramite siti *web* malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Remote Administration Tool **(RAT)**. Si tratta, letteralmente, di strumenti di amministrazione remota di *server* o postazioni di lavoro, ossia di una funzionalità che permette all'amministratore del sistema o all'utente di accedere da remoto alla macchina e di eseguire operazioni sulla stessa.

Spear phishing. Attacco informatico di tipo *phishing* condotto contro utenti specifici mediante l'invio di *e-mail* formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o *link* malevoli.

SQL Injection. Tecnica mirata a colpire applicazioni *web* che si appoggiano su database programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in *input* e l'inserimento di codice malevolo all'interno delle *query*. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

Supervisory Control and Data Acquisition **(SCADA)**. Gli SCADA sono una tipologia dei sistemi di controllo industriale. Si tratta di sistemi informatici distribuiti per il monitoraggio ed il controllo elettronico, centralizzato, di infrastrutture cd. *cyber*-fisiche, tra loro anche geograficamente lontane, tipicamente utilizzati in ambito industriale, ovvero da infrastrutture critiche.

Trojan. *Malware* che impiega l'ingegneria sociale, presentandosi come un file legittimo (ad esempio con estensione .doc o .pdf), facendo credere alla vittima che si tratti di un file innocuo, ma che in realtà cela un programma che consente l'accesso non autorizzato al sistema da parte dell'attaccante. Il *trojan* può avere diverse funzioni: dal furto di dati sensibili al danneggiamento del sistema target. Particolare categoria sono i cd. ***Banking Trojan***, , programmati per acquisire le credenziali di accesso degli *account* dei siti di banca *on-line* al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di *cyber* criminali.

Underground. Con tale termine si intende l'ambiente, solitamente digitale, frequentato per l'acquisto o la condivisione di strumenti di *hacking*.

Watering-hole. Particolare tipologia di attacco in cui l'attore ostile individua, sulla base di attività di osservazione e profilazione del *target*, i siti *web* di interesse della vittima e li infetta con *malware*, così da poter colpire indirettamente l'obiettivo. Tale strategia si rivela particolarmente utile laddove non sia possibile diffondere il *malware* tramite *spear phishing*.

Web-defacement. Attacco condotto contro un sito *web* e consistente nel modificare i contenuti dello stesso limitatamente alla *home-page* ovvero includendo anche le sottopagine del sito.